



Obteniendo el Token #1

Transcripción

[00:00] Bien, ya tenemos la primera parte completa, ya tenemos nuestro filtro implementado y ya estamos pasando el request al siguiente nivel para el Controller. ¿Qué es lo que sigue? Exacto. Lo que sigue en nuestro flujo de autorización, ya estamos aquí, ahora lo que vamos a hacer es validar el token.

[00:19] ¿Cómo lo vamos a hacer? Venimos aquí y tenemos que ver principalmente dos cosas. La primera, yo aquí tengo que obtener el token, y esto lo voy a obtener de los headers. ¿Cómo es que esto va a llegar? Observen, por ejemplo, aquí en mi cliente, que es Insomnia, yo tengo aquí una pestaña de autenticación que es esta de acá.

[00:43] Si voy a mi registrar médicos también, por ejemplo, tienen Auth, en actualizar tienen Auth, y esto es para los tipos de autenticación que podemos implementar, por ejemplo, en mi listado yo puedo elegir entre tener no autenticación, tenerlo libre, completamente vacío, o también puedo implementar un API security key, para hacer la autenticación o OAuth, usar Bearer Token, que es nuestro caso.

[01:11] Y automáticamente pues Insomnia me va a proveer un campo para el token y un campo para el prefijo. El prefijo lo vamos a ver un momento, todavía no se preocupen, vamos a comenzar por el token. Primero necesito generar otro token válido porque este token lo he generado hace unos días, voy a darle enviar otra vez y ya me genera otro token. Voy a copiar este token aquí.

[01:35] Le damos "Ctrl + C", venimos a nuestro listado y aquí yo le voy a decir "Mándame el token en el header" y prefijo lo voy a dejar vacío por ahora. Van a ver qué se trata de este parámetro en un momento más. Volvemos al código y ahora tengo que obtener el token que estoy enviando aquí que va a llegar en un header. Tengo que ir obtenerlo aquí.

[01:59] Si voy a la parte de headers, puedes ver que yo no estoy agregando ningún header personalizado, entonces vamos a ver cómo lo puedo hacer. Normalmente por standard el token llega en un header específico, que es authorization. El nombre del header, donde llega el token JWT es authorization.

[02:29] Entonces lo que vamos a hacer aquí es este request.getHeader, es un método. Esto me va a decir cómo se llama el header, se llama "Authorization" que es autorización en inglés, punto y coma, y aquí yo quiero imprimir el token, para ver si es que estoy logrando obtener el token que yo quiero.

[02:52] Entonces este es mi primer paso, hacer un request.getHeaderAuthorization e imprimir el token y después sigue la vida y pasamos al siguiente filtro, vamos a ver si funciona, vamos a guardar primero. Vemos que ya reinició, perfecto. Enviamos, vemos qué pasó, vemos aquí a headers, no vemos ningún header en la respuesta.

[03:16] Vamos aquí, vemos que se sucedió el query y observen acá. Observen este token de aquí. Es el mismo token que hemos enviado aquí en nuestro header de autorización, authorization, ya estamos con esto, pero miren el prefijo que hay aquí: el bearer.

[03:36] Este bearer viene a ser el prefijo que por defecto en el estándar ya está especificado así. Por estándar este token siempre va a tener el prefijo bearer y después va a seguir el token. Entonces como yo solamente quiero trabajar con mi token, lo que voy a hacer aquí es .replace y le voy a decir que yo quiero reemplazar "Bearer" más el espacio, coma, por vacío.

[04:10] Entonces mi token lo que va hacer es retornar el header de autorización y reemplazar el parámetro “Bearer” por nada, por vacío. Entonces lo único que me va a retornar es mi token en sí, mi token específico y es lo único que yo necesito para esto. Entonces, vamos a ver si aquí reinicio mi servidor. Voy a enviar otra vez el request.

[04:33] Voy a ver aquí y listo está funcionando. Yo tengo esto aquí. Por ejemplo, nuevamente recuerden el nombre del header en específico, es authorization. Si yo pongo por ejemplo authorizations o cualquier cosa, esto me va a dar un error, me va a dar una excepción, porque va a lanzar un null pointer exception. Es lo más probable.

[04:55] Vamos a probar aquí. Enviamos otra vez. Me dio un 500. ¿Por qué? Porque simplemente este header no existe, el estándar ya te dice que es authorization en singular, y ese es el nombre, a no ser que por reglas del negocio hayan definido, que el nombre va a ser diferente, pero eso ya sería una mala práctica porque estarían yendo en contra del estándar.

[05:20] Entonces, sin más, ya tenemos el token, ya tenemos la primera parte. Miren, tenemos el token. Estamos obteniendo el header de autorización y estamos reemplazando la parte Bearer, el prefijo “Bearer” por vacío para obtener el token en sí. ¿Qué es lo que sigue? ¿Qué tenemos que hacer? Tenemos que comenzar a evaluar si el token es válido, no es válido, si es este usuario, si no es de este usuario.

[05:43] Entonces quédense aquí. Quizás es un poquito complicado al inicio, no se preocupen. Esto es hasta un poco más simple que nuestro proceso de autenticación. Entonces nos vemos en el siguiente video para implementar ya la validación en sí.

